

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-174441

(43)Date of publication of application : 20.06.2003

(51)Int.Cl.

H04L 9/08
H04L 9/14

(21)Application number : 2001-371463

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 05.12.2001

(72)Inventor : ANDO DAISUKE
YUKI NAOHIKO
SATO TAKAKO

(54) CONTENTS ENCRYPTING METHOD AND DEVICE AND CONTENTS DECODING METHOD AND DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To realize encryption corresponding to multi-cast for changing a cryptographic key in every second order, and for facilitating countermeasures to terminal equipment whose processing capability is low in distributing the contents of an IP stream or the like.

SOLUTION: An encrypting server 2 encrypts and transmits a cryptographic key (key array) K_{cn} for encrypting the IP stream to a terminal 3 in each transmission interval of a prescribed cryptographic key, and encrypts and transmits the packet of the IP stream by using one cryptographic key K_{cn} in each prescribed encryption interval. Also, the encrypting server 2 encrypts and transmits the updated new cryptographic key (key array) K_{cn} to the terminal 3 in each update interval of the prescribed cryptographic key. When the received packet are data, the terminal 3 decodes the packet by one cryptographic key (key array) K_{cn} , and when the packet are associated with the cryptographic key, the terminal 3 decodes and stores the packet.

